Index

[5 Organizational controls 4](#_Toc151391684)

[5.1 Policies for information security 4](#_Toc151391685)

[5.2 Information security roles and responsibilities 4](#_Toc151391686)

[5.3 Segregation of duties 4](#_Toc151391687)

[5.4 Management responsibilities 4](#_Toc151391688)

[5.5 Contact with authorities 4](#_Toc151391689)

[5.6 Contact with special interest groups 4](#_Toc151391690)

[5.7 Threat intelligence 4](#_Toc151391691)

[5.8 Information security in project management 4](#_Toc151391692)

[5.9 Inventory of information and other associated assets 4](#_Toc151391693)

[5.10 Acceptable use of information and other associated assets 4](#_Toc151391694)

[5.11 Return of assets 4](#_Toc151391695)

[5.12 Classification of information 4](#_Toc151391696)

[5.13 Labelling of information 4](#_Toc151391697)

[5.14 Information transfer 4](#_Toc151391698)

[5.15 Access control 5](#_Toc151391699)

[5.16 Identity management 5](#_Toc151391700)

[5.17 Authentication information 5](#_Toc151391701)

[5.18 Access rights 5](#_Toc151391702)

[5.19 Information security in supplier relationships 5](#_Toc151391703)

[5.20 Addressing information security within supplier agreements 5](#_Toc151391704)

[5.21 Managing information security in the ICT supply Chain 5](#_Toc151391705)

[5.22 Monitoring, review and change management of supplier services 5](#_Toc151391706)

[5.23 Information security for use of cloud services 5](#_Toc151391707)

[5.24 Information security incident management planning and preparation 5](#_Toc151391708)

[5.25 Assessment and decision on information security events 5](#_Toc151391709)

[5.26 Response to information security incidents 5](#_Toc151391710)

[5.27 Learning from information security incidents 5](#_Toc151391711)

[5.28 Collection of evidence 5](#_Toc151391712)

[5.29 Information security during disruption 5](#_Toc151391713)

[5.30 ICT readiness for business continuity 6](#_Toc151391714)

[5.31 Legal, statutory, regulatory and contractual requirements 6](#_Toc151391715)

[5.32 Intellectual property rights 6](#_Toc151391716)

[5.33 Protection of records 6](#_Toc151391717)

[5.34 Privacy and protection of PII 6](#_Toc151391718)

[5.35 Independent review of information security 6](#_Toc151391719)

[5.36 Compliance with policies, rules and standards for information security 6](#_Toc151391720)

[5.37 Documented operating procedures 6](#_Toc151391721)

[6 People controls 6](#_Toc151391722)

[6.1 Screening 6](#_Toc151391723)

[6.2 Terms and conditions of employment 6](#_Toc151391724)

[6.3 Information security awareness, education and training 6](#_Toc151391725)

[6.4 Disciplinary process 6](#_Toc151391726)

[6.5 Responsibilities after termination or change of employment 6](#_Toc151391727)

[6.6 Confidentiality or non-disclosure agreements 6](#_Toc151391728)

[6.7 Remote working 6](#_Toc151391729)

[6.8 Information security event reporting 7](#_Toc151391730)

[7 Physical controls 7](#_Toc151391731)

[7.1 Physical security perimeters 7](#_Toc151391732)

[7.2 Physical entry 7](#_Toc151391733)

[7.3 Securing offices, rooms and facilities 7](#_Toc151391734)

[7.4 Physical security monitoring 7](#_Toc151391735)

[7.5 Protecting against physical and environmental threats 7](#_Toc151391736)

[7.6 Working in secure areas 7](#_Toc151391737)

[7.7 Clear desk and clear screen 7](#_Toc151391738)

[7.8 Equipment siting and protection 7](#_Toc151391739)

[7.9 Security of assets off-premises 7](#_Toc151391740)

[7.10 Storage media 7](#_Toc151391741)

[7.11 Supporting utilities 7](#_Toc151391742)

[7.12 Cabling security 7](#_Toc151391743)

[7.13 Equipment maintenance 7](#_Toc151391744)

[7.14 Secure disposal or re-use of equipment 7](#_Toc151391745)

[8 Technological controls 8](#_Toc151391746)

[8.1 User endpoint devices 8](#_Toc151391747)

[8.2 Privileged access rights 8](#_Toc151391748)

[8.3 Information access restriction 8](#_Toc151391749)

[8.4 Access to source code 8](#_Toc151391750)

[8.5 Secure Authentication 8](#_Toc151391751)

[8.6 Capacity management 8](#_Toc151391752)

[8.7 Protection against malware 8](#_Toc151391753)

[8.8 Management of technical vulnerabilities 8](#_Toc151391754)

[8.9 Configuration management 8](#_Toc151391755)

[8.10 Information deletion 8](#_Toc151391756)

[8.11 Data masking 9](#_Toc151391757)

[8.12 Data leakage prevention 9](#_Toc151391758)

[8.13 Information backup 9](#_Toc151391759)

[8.14 Redundancy of information processing facilities 9](#_Toc151391760)

[8.15 Logging 9](#_Toc151391761)

[8.16 Monitoring activities 9](#_Toc151391762)

[8.17 Clock synchronization 9](#_Toc151391763)

[8.18 Use of privileged utility programs 9](#_Toc151391764)

[8.19 Installation of software on operational systems 9](#_Toc151391765)

[8.20 Networks security 9](#_Toc151391766)

[8.21 Security of network services 9](#_Toc151391767)

[8.22 Segregation of networks 9](#_Toc151391768)

[8.23 Web filtering 9](#_Toc151391769)

[8.24 Use of cryptography 9](#_Toc151391770)

[8.25 Secure development life cycle 9](#_Toc151391771)

[8.26 Application security requirements 9](#_Toc151391772)

[8.27 Secure system architecture and engineering principles 10](#_Toc151391773)

[8.28 Secure coding 10](#_Toc151391774)

[8.29 Security testing in development and acceptance 10](#_Toc151391775)

[8.30 Outsourced development 10](#_Toc151391776)

[8.31 Separation of development, test and production environments 10](#_Toc151391777)

[8.32 Change management 10](#_Toc151391778)

[8.33 Test information 10](#_Toc151391779)

[8.34 Protection of information systems during audit testing 10](#_Toc151391780)

# 5 Organizational controls

## 5.1 Policies for information security

Does not apply.

## 5.2 Information security roles and responsibilities

Does not apply.

## 5.3 Segregation of duties

Does not apply.

## 5.4 Management responsibilities

Does not apply

## 5.5 Contact with authorities

Does not apply

## 5.6 Contact with special interest groups

Does not apply

## 5.7 Threat intelligence

Does not apply

## 5.8 Information security in project management

Does not apply

## 5.9 Inventory of information and other associated assets

Does not apply

## 5.10 Acceptable use of information and other associated assets

Does not apply

## 5.11 Return of assets

Does not apply

## 5.12 Classification of information

Does not apply (Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements)

## 5.13 Labelling of information

Does not apply

## 5.14 Information transfer

Does not apply

## 5.15 Access control

Does not apply

## 5.16 Identity management

Does not apply

## 5.17 Authentication information

Does not Apply

## 5.18 Access rights

Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control. It could be amplified in detail, review guidance section.

## 5.19 Information security in supplier relationships

Does not apply

## 5.20 Addressing information security within supplier agreements

Does not apply

## 5.21 Managing information security in the ICT supply Chain

Does not apply

## 5.22 Monitoring, review and change management of supplier services

Does not apply

## 5.23 Information security for use of cloud services

Does not apply

## 5.24 Information security incident management planning and preparation

Does not apply

## 5.25 Assessment and decision on information security events

Does not apply

## 5.26 Response to information security incidents

Does not apply

## 5.27 Learning from information security incidents

Does not apply

## 5.28 Collection of evidence

The organization should establish and implement procedures for the identification, collection,

acquisition and preservation of evidence related to information security events (LOGS, auditing)

## 5.29 Information security during disruption

Does not apply

## 5.30 ICT readiness for business continuity

Does not apply

## 5.31 Legal, statutory, regulatory and contractual requirements

Does not apply.

## 5.32 Intellectual property rights

Does not apply

## 5.33 Protection of records

Does not apply

## 5.34 Privacy and protection of PII

Does not apply

## 5.35 Independent review of information security

Does not apply

## 5.36 Compliance with policies, rules and standards for information security

Does not apply

## 5.37 Documented operating procedures

Does not apply

# 6 People controls

## 6.1 Screening

Does not apply

## 6.2 Terms and conditions of employment

Does not apply

## 6.3 Information security awareness, education and training

Does not apply

## 6.4 Disciplinary process

Does not apply

## 6.5 Responsibilities after termination or change of employment

Does not apply

## 6.6 Confidentiality or non-disclosure agreements

Does not apply

## 6.7 Remote working

Does not apply

## 6.8 Information security event reporting

Does not apply

# 7 Physical controls

## 7.1 Physical security perimeters

Does not apply

## 7.2 Physical entry

Does not apply

## 7.3 Securing offices, rooms and facilities

Does not apply

## 7.4 Physical security monitoring

Does not apply

## 7.5 Protecting against physical and environmental threats

Does not apply

## 7.6 Working in secure areas

Does not apply

## 7.7 Clear desk and clear screen

Does not apply

## 7.8 Equipment siting and protection

Does not apply

## 7.9 Security of assets off-premises

Does not apply

## 7.10 Storage media

Does not apply

## 7.11 Supporting utilities

Does not apply

## 7.12 Cabling security

Does not apply

## 7.13 Equipment maintenance

Does not apply

## 7.14 Secure disposal or re-use of equipment

Does not apply

# 8 Technological controls

## 8.1 User endpoint devices

Information stored on, processed by or accessible via user endpoint devices should be protected.

## 8.2 Privileged access rights

Control: The allocation and use of privileged access rights should be restricted and managed.

Purpose: To ensure only authorized users, software components and services are provided with privileged access rights.

## 8.3 Information access restriction

Control: Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.

Purpose: To ensure only authorized access and to prevent unauthorized access to information and other associated assets.

## 8.4 Access to source code

Does not apply.

## 8.5 Secure Authentication

Control: Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.

Purpose: To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.

Guidance: A suitable authentication technique should be chosen to substantiate the claimed identity of a user, software, messages and other entities.

## 8.6 Capacity management

Does not apply

## 8.7 Protection against malware

Does not apply

## 8.8 Management of technical vulnerabilities

Does not apply.

## 8.9 Configuration management

Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed (It could be included to fortify the need for implementing security configurations by file codes)

## 8.10 Information deletion

Does not apply.

## 8.11 Data masking

Does not apply.

## 8.12 Data leakage prevention

Does not apply

## 8.13 Information backup

Does not apply

## 8.14 Redundancy of information processing facilities

Does not apply

## 8.15 Logging

Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analyzed. (It could be used for logging and auditing)

## 8.16 Monitoring activities

Does not apply

## 8.17 Clock synchronization

Does not apply

## 8.18 Use of privileged utility programs

Does not apply

## 8.19 Installation of software on operational systems

Does not apply

## 8.20 Networks security

Does not apply

## 8.21 Security of network services

Does not apply

## 8.22 Segregation of networks

Does not apply

## 8.23 Web filtering

Does not apply

## 8.24 Use of cryptography

Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.

## 8.25 Secure development life cycle

Does not apply

## 8.26 Application security requirements

Does not apply

## 8.27 Secure system architecture and engineering principles

Does not apply

## 8.28 Secure coding

Does not apply

## 8.29 Security testing in development and acceptance

Does not apply.

## 8.30 Outsourced development

Does not apply.

## 8.31 Separation of development, test and production environments

Does not apply.

## 8.32 Change management

Does not apply.

## 8.33 Test information

Does not apply.

## 8.34 Protection of information systems during audit testing

Does not apply.